100TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPT. 100-153
Part 1

COMPUTER SECURITY ACT OF 1987

JUNE 11, 1987.—Ordered to be printed

Mr. ROE, from the Committee on Science, Space, and Technology, submitted the following

REPORT

[To accompany H.R. 145 which on January 6, 1987, was referred jointly to the Committee on Science, Space, and Technology and the Committee on Government Operations]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 145) to provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal Computer systems, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

		Page
I.	Background	6
II.	Issues raised during the hearings	9
III.	Need for legislation	22
IV.	Explanation of the bill	23
V.	Sectional analysis	31
VI.	Effect of legislation on inflation	37
VII.	Committee oversight findings and recommendation	37
VIII.	Oversight findings and recommendations by the Committee on Government Operations	37
IX.	Budget analysis and projection	37
X.	Congressional Budget Office cost estimate	37
XI.	Administration position	41
XII.	Changes in existing law made by the bill, as reported	41
XIII.	Committee recommendation	47

The amendment is as follows:

74-018

H703-8

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

The Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901, (15 U.S.C. 271-278h), is amended—

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

"SEC. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code.

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of

this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

"(3) by adding at the end thereof the following new section:

"SEC. 23. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Oper-

ations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude or the harm resulting from the loss,

misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

I. BACKGROUND

Computers and information systems have so permeated today's society that there is virtually no sector which does not rely heavily on their use. This includes the Federal Government, which currently has over 17,000 medium- and large-scale computers and will have almost 500,000 microcomputers by 1990, according to a 1985 report by the General Services Administration, entitled "ADP Management of Information Systems".

The Federal Government is the largest single user of computers in the world. Its investment in automated systems technology is so large that about 1.6 percent of the 1986 budget was spent on automated data processing (ADP) equipment and services, or more than 15 billion dollars. This budget included ADP for defense and national security, education, national energy programs, social welfare, and tax programs.

As the role of the Federal Government has become broader, the need to automate and the corresponding need to secure data also has grown. In recent years, Congress and the executive agencies have directed their attention to Federal computer systems in a number of areas, including investigating and commenting on their integrity and security. Both Section 111(f) of the Federal Property and Administrative Service Act of 1949 (as amended by the Brooks Act of 1965) and the Paperwork Reduction Act of 1980 represented attempts by Congress to address the issues of automating information in Federal agencies and creating an efficient method of storing and disseminating this information. In October 1984, Congress passed the first Federal computer crime legislation, the Counterfeit Access Device and Computer Fraud Act of 1984 (P.L. 98-473). That law has been amended by the Computer Fraud and Abuse Act of 1986 (P.L. 99-474). This law prohibited "unauthorized access" into "Federal interest computers" affecting national security data, financial data, and other data stored in these computers. In addition, penalties were established for pirated "bulletin boards" containing

information which might lead to the fraud or abuse of data in a computer.

Within the Federal Government several agencies have been charged with the responsibility for establishing computer security controls and standards. The Office of Management and Budget (OMB) has overall responsibility for computer security policy. The General Services Administration (GSA) also issues regulations for physical security of computer facilities, and ensures that security hardware and software meet certain technological and fiscal specifications. In defense and national security, the National Security Agency (NSA) has traditionally been responsible for the security of classified information, including that processed by and stored within computers. Recently, NSA has been given the responsibility to establish and maintain technical standards for secure, or "trusted," computers. NSA does this through its administration of the Department of Defense (DOD) National Computer Security Center. NSA also will work with industries at the DOD Computer Security Center to develop security standards for private sector use.

At the Department of Commerce, the National Bureau of Standards' (NBS) Institute of Computer Science and Technology (ICST) has developed computer and processing standards, such as the Data Encryption Standard (DES), which protects data transferred between automated information systems. The Federal Information Processing Standards (FIPS) developed by the ICST provide specific codes, language, procedures, and techniques for Federal and private sector information systems managers. Also at the Department of Commerce, the National Telecommunications and Information Administration (NTIA) has the responsibility for analyzing, developing, implementing and applying executive branch policy for telecommunications in the Federal Government.

CURRENT FEDERAL ROLE

This mixture of laws, regulations, and responsible agencies has raised concern that Federal computer security policy is lacking direction and forcefulness in some areas, yet has created overlapping and duplication of effort in other areas. Recently, Federal regulations and directives have been issued and congressional legislation has been introduced to address the lack of coordination of Federal ADP systems.

On March 15, 1985, OMB issued a draft circular intended "to provide a general framework of management of information resources." This circular combined and updated previous OMB circulars, including OMB Circular A–71 (originally issued in July 1978). The final OMB circular, A130, was issued on December 12, 1985. Appendix III of the circular addressed Federal Government computer security. Those responsible for implementing of this circular include the Department of Commerce, Department of Defense, General Services Administration, and the Office of Personnel Management, in addition to OMB.

On September 17, 1984, the executive branch issued National Security Decision Directive 145 (NSDD–145), "National Policy on Telecommunications and Automated Information Systems Security". This directive is aimed at safeguarding automated information

systems with a special focus on protecting those Federal systems accessed via (and dependent on) network communications. NSDD-145 creates a National Telecommunications and Information Systems Security Committee (NTISSC), a panel of 22 voting representatives from 12 defense/intelligence agencies and 10 civilian agencies. An Assistant Secretary of Defense chairs NTISSC, and the Director of the National Security Agency acts as the National Manager for implementing policy under NSDD-145. The NTISSC is empowered to issue operating policies to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive information.

On June 27, 1985, Representative Dan Glickman, then chairman of the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, introduced H.R. 2889, the Computer Security and Training Act of 1985. The intent of this legislation was to establish NBS as the focal point for developing training guidelines for Federal employees who are involved in management, operation, and use of automated information processing systems. This legislation was based in part on hearings which the subcommittee conducted in 1983 and a 1984 subcommittee report which had recommended increased ADP training and awareness in Federal agencies. The Subcommittee on Transportation, Aviation and Materials held hearings on H.R. 2889 on September 24, 1984, June 27, 1985, and October 29 and jointly with the Subcommittee on Science, Research and Technology on October 30, 1985. At the end of the 99th Congress, under House procedures, the bill was brought up for consideration under suspension of rules, the bill failed to obtain the two-thirds vote required and the bill went no further.

On October 29, 1986, National Security Adviser John Poindexter issued National Telecommunications Information Systems and Security (NTISS) policy Directive No. 2. This directive would have added a new "sensitive but unclassified" category of Federal information, setting new classification criteria for information formerly unclassified. It would not only have affected managers, users, and programmers of information systems within the Federal Government, but there was concern that it could have been extended to private sector contractors of the Federal Government as well, potentially restricting the type of information and data released. However, on March 16, 1987, National Security Adviser Frank Carlucci rescinded NTISS Directive No. 2, following negotiations with the committees having jurisdiction over H.R. 145.

On January 6, 1987, Representative Dan Glickman introduced H.R. 145, the Computer Security act of 1987. This legislation, based in part on H.R. 2889 introduced during the 99th Congress would assign the National Bureau of Standards responsibility for developing standards and guidelines for the security of Federal computer systems, drawing upon technical guidelines developed by the National Security Agency, when such guide lines are consistent with the requirements for protecting sensitive information. H.R. 145 also provides for a Computer Systems Advisory Board to identify emerging Federal computer security and privacy issues, advise NBS on these issues, report its findings to the Office of Management and

Budget (OMB), NSA, and Congress. The bill also would amend the Brooks Act of 1965 by updating the term "computer"; require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

II. Issues Raised During the Hearings

During the 99th Congress, the Subcommittee on Transportation, Aviation and Materials held hearings on Federal computer and communications privacy and security on September 24, 1984, June 27, 1985, and October 29 and jointly with the Subcommittee on Science, Research and Technology on October 30, 1985. During the 100th Congress, the Subcommittee on Transportation, Aviation, and Materials, and the Subcommittee on Science, Research and Technology of the House Science, Space, and Technology Committee held hearings on H.R. 145 on February 26, 1987. The Subcommittee on Transportation, Aviation, and Materials held an additional hearing on May 19, 1987, before final consideration of H.R. 145 by the full House Science, Space, and Technology Committee.

These hearings touched upon four major issues: (1) the current state of computer security in the Federal Government; (2) the role of the National Security Agency (NSA) in setting Federal computer security; (3) the issue of privacy and security, particularly with a new "sensitive but unclassified" criteria; and (4) the role of the Federal Government in adequately training Federal employees and heightening awareness of computer security.

FEDERAL COMPUTER CRIME AND SECURITY

99th Congress

Over the course of the 99th Congress, there was a heightened awareness both inside and outside the Federal Government that current computer security measures were inadequate. The American Bar Association, the Inspector General's Office of the Department of Health and Human Services, computer crime experts such as Donn Parker, and industry representatives have repeatedly cited the lack of management, controls, and coordination of computer security in both the private sector and in the Federal Government.

During the September 24, 1984 hearings, John Tompkins, chairman of the Task Force on Computer Crime of the American Bar Association (ABA), commented on a survey conducted by the ABA on the state of computer crime in government and the private sector. The ABA report was one of the first extensive studies done on the number of "known and verifiable losses" which have resulted from computer crimes, and the results of the survey included responses from 13 Federal agencies and 28 State and local agencies. Although the results of the survey indicated a wide range of losses by respondents, several consistent factors emerged: that "insiders" having access to computer systems are the more likely perpetrators of fraud and abuse; that there is a proliferation of computers in government; that such security systems as currently exist do not

facilitate detection of computer crimes; that security systems themselves often are vulnerable and inadequate; and that a lack of awareness and concern by the public as well as computer systems managers, are contributing to these problems. Mr. Tompkins noted that, although the ABA did not state any formal recommendations, the conclusions reached by the respondents to the ABA survey indicated: the need for Federal computer crime legislation; the need to adequately train and supervise personnel in data processing; and the large overall cost and expense of computer fraud and abuse.

Richard Kusserow, Inspector General for the Department of Health and Human Services, also testified on the nature of fraud and abuse in Federal computer systems. As Inspector General for the largest Federal civil agency, Mr. Kusserow's office has been involved with auditing computer systems, reducing costs, and insuring the integrity of HHS ADP systems. As Mr. Kusserow stated at the September 24 hearings:

> We must ensure that agency managers in overseeing programs that use computerized systems, do audit the systems, do look and make sure that the controls are functioning, and that we in the inspector general community, using our auditors and investigators, follow up to make sure it's being done. I think that in all of these areas it has not been done nearly enough.

Also, as chairman of the President's Council on Integrity and Efficiency investigating computer crime in the Federal Government, Mr. Kusserow testified on September 24, 1984, and again on October 29, 1985, on a study he directed which examined computer-related fraud and abuse in general, and a subsequent study in which the Inspector General's office interviewed those who had been convicted of Federal computer fraud and abuse. The results of these studies are consistent with the findings of the ABA study: that Federal computer fraud and abuse is often committed by insiders within the Federal agency; that training for computer security and awareness of vulnerabilities in computer systems were lacking; and that internal controls for computer security need to be increased. The profile of Federal computer criminals shows that they are young, considered good employees, and often use co-conspirators, and that many who commit these crimes never think about the consequences of being caught, or if they consider the consequences, assess the risk of being caught as minimal. As Mr. Kusserow stated in the October 29, hearing:

> One of the most disturbing findings from this study is that the work environment provided the perpetrators with the opportunity to commit their crime. We asked the perpetrators about computer security where they had committed their crime . . . Virtually all of them had been aware of security efforts but most said they has been weak. So, they make the judgment that, although there may have been security efforts in their agencies, they were weak and could not be counted upon to act as a deterrence for them to committing the crime.

The General Accounting Office also testified during the hearings on June 27, 1985, and October 29 and 30, 1985. GAO has conducted several studies on a computer crime and security in the Federal Government, including a 1985 survey of 25 computer systems in 17 Federal civil agencies, to evaluate the state of computer security and integrity of these systems. This survey was conducted by GAO using two questionnaires and subsequent interviews, promising anonymous to the agencies so the systems could not be compromised after public disclosure. GAO indicated that:

> Generally, the results of our survey showed that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste. Specifically we found that: key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program; and actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques, such as passwords, allowing access to systems were not periodically changed.

GAO categorized Federal computer security methods into management and three basic safeguard components: physical, technical, and administrative. No agency met all of the management responsibilities outlined in the questionnaire, and only five of the 25 systems evaluated contained an element of physical, technical and administrative control. Only two of the systems provide what GAO described as adequate training for computer employees. GAO further characterized the systems as very vulnerable, and given the minimal oversight and coordination between agencies, GAO found that there is a lack of a balanced approach to security of Federal computer systems.

The testimony by the ABA, the Inspector General's office of HHS, and GAO clearly indicated that Federal systems are in danger because of improper use and negligence. Other witnesses from both the public and private sector testified during the hearings that they also found computer security in general and Federal computer security specifically remains vulnerable and open to fraud and abuse, despite stated efforts by representatives of the Federal agencies to remedy this problem.

100th Congress

After the hearings on H.R. 2889 during the 99th Congress, the House Science and Techology Committee requested that GAO review how successfully appropriate security controls are being incorporated into mission-critical, sensitive systems now being developed in Federal civilian agencies. GAO proceeded to evaluate nine Federal civilian agencies to determine the effectiveness of computer security controls.

GAO evaluators determined during the course of this study that currently there is a lack of effective guidance for assessing whether appropriate security controls are initiated during the development of computer systems. None of the nine agencies reviewed treated information security as one of its functional requirements. According to GAO, six of the nine agencies studied did not address, or in-

adequately addressed, the sensitivity of the information to be handled in a computer system. Eight of the nine agencies performed no risk analysis of the computer systems in the agency.

Thomas B. Giammo, Associated Director, Information Management and Technology Division of GAO stated during testimony:

> Mr. Chairman, our review suggests that the practices currently being used by civilian agencies in the development of mission-critical, sensitive systems will not assure that the appropriate security controls are being successfully incorporated into these systems. Specifically, we reviewed the practices currently being used at nine civilian agencies in the development of nine specific systems. We found that the practices in use at all nine agencies had permitted decisions cirtical to the specification, design, and construction of all nine systems to be made without adequate management consideration of important security issues.

This evaluation of Federal civilian agencies' lack of computer security planning and management supports the previous GAO study on Federal civilian agency computer security. It also corroborates testimony from other witnesses during hearings on H.R. 145 regarding the need for incorporating security controls into mission-sensitive critical computer systems.

ROLE OF THE NATIONAL SECURITY AGENCY (NSA)

With the introduction of NSDD-145, the prominent role of the NSA in establishing Federal computer security in civilian agencies became a subject of debate among computer security experts. The Subcommittee on Transportation, Aviation and Materials devoted an entire day of hearings to this subject on June 27, 1985, during which representatives from NSA and DOD testified. The role of NSA under NSDD-145 was a topic mentioned during the hearings on October 29 and 30, 1985. The role of NSA under NSDD-145 was further examined during hearings on H.R. 145 on February 26, 1987.

99th Congress

Donald Latham, Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC), Walter Deeley, Deputy Director for Communications Security, NSA, and Robert Brotzman, Director, DOD National Computer Security Center, testified on why NSDD-145 was necessary to coordinate Federal computer security. Citing a lack of overall coordination among Federal agencies, the high risk of compromising, losing or destroying Federal agency data, and the overall vulnerability of Federal computer security systems, they emphasized that the NSA had the experience and expertise to administer Federal computer security programs. As Mr. Latham stated:

> We have provided cryptographic devices for protection of classified data, as Mr. Deeley will explain further. While we have done a reasonable job in some areas, there are

> still many areas that are left uncovered and there is more emphasis needed here.
>
> We have put in controls for tighter access to unclassified data through network access controls and things like this, so that the so-called hackers can't go in and just play havoc with our data.
>
> We are fostering very much a security awareness program. We are instituting training programs at the national level as well as the local level, I'll say, within service schools and across the various agencies. And we are looking at more rigorous ways of clearing people who have access to computer systems and telecommunications network security devices.

Other witnesses appearing before the subcommittee expressed concerns that NSDD-145 would hamper efforts to adequately administer Federal computer security. One area of concern is that NSDD-145 will create conflict with other Federal security regulations, notably Transmittal Memorandum 1 to OMB Circular A-71 (which has since been embodied in OMB Circular A-130, published December 12, 1985). Although both NSDD-145 and the OMB circular are broadly constructed, the emphasis in the OMB circular for planning and implementing Federal computer security rests with civil agencies, primarily with OMB and the Department of Commerce. In NSDD-145, the Director of NSA and the Secretary of Defense have primary roles. NSDD-145 does incorporate many of the lead Federal agencies on its NTISSC panel; but not all agencies are included. When Warren Reed, Director, Information Management and Technology Division, General Accounting Office, testified on the GAO survey on Federal computer security, he stated that the issuance of NSDD-145 might create confusion among the Federal agencies over which agency has jurisdiction over security functions. Mr. Reed stated that this could be a large or small problem, and may interfere with other Federal statutes and regulations which have given this jurisdiction to NBS. Raymond Wyrsch, Senior Attorney, Office of General Counsel at GAO, stated:

> * * * we do have laws on the books, the Brooks Act and the Paperwork Reduction Act, and there are very distinct responsibilities that have been placed on these agencies, namely OMB has been given the general oversight authority, if you will to set government policy.
>
> * * * And I don't know if anyone is really in the position to say with any degree of conclusiveness now, on what are the other agencies supposed to do if you have inconsistent or conflicting guidance that may be issued. There have been various pronouncements that have been made by the Secretary of Commerce over the years dealing with ADP standards.

Representative Jack Brooks, Chairman of the Subcommittee on Legislation and National Security of the House Government Operations Committee, and author of the Brooks Act, highlighted these concerns during his testimony on NSDD-145: "NSA has a propensity and a tendency to classify everything." GAO witnesses also ex-

pressed concern that a lack of definition of "unclassified information considered sensitive" in civil agencies may be interpreted either broadly or narrowly, significantly affecting how agencies store and disseminate information contained in computer and telecommunications systems. However, Lt. Gen. Odom, Director of NSA, has stated in a letter to Chairman Fuqua on February 25, 1986: ". . . the Systems Steering Group, the senior governmental body created by NSDD-145 for information security matters, has concluded that each government department or agency must make its own determination as to what constitutes sensitive information to that department or agency mission or operation."

Other witnesses, including representatives from the American Civil Liberties Union and the Institute of Electrical and Electronics Engineers, expressed similar concerns over the "unclassified but sensitive" categorization of computerized data and how that will affect citizens' access to public information or freedom to exchange scientific information.

There has been some controversy over the review process for NSDD-145. Expressing concern that issuing National Security Decision Directive 145 effectively circumvents the review process that OMB Circular A-71 went through, Subcommittee Chairman Glickman noted during testimony given on June 27, that a document which ordinarily might be called a regulation, if labeled a national security directive, may avoid the Administrative Procedures Act, all public notification requirements, and Congressional oversight. Also, Mr. Richard P. Kusserow, Inspector General of HHS, stated at the October 29 hearing that "I haven't seen it, and I have not had any imput in the process". Still the review process spanned nearly a year and Dr. Robert E. Conley, who was chairman of the Subgroup on Telecommunications Security created under NSDD-145 while he was with the Treasury Department, said at the same hearing that "we invited all of the government agencies to attend the meetings". Thus, although there is no question that Federal computer security is a vital national issue, use of NSDD-145 as an instrument for setting policy, without legislative or agency debate and review, has raised concerns in the Congress.

100th Congress

During the 100th Congress, the debate regarding NSDD-145 and the role of NSA in setting computer security policy for Federal civilian agencies has continued. H.R. 145 states that the responsibility for developing standards and guidelines for the security and privacy of Federal computer systems rests with NBS, with technical advice and assistance coming from NSA "where appropriate". The hearings before the Subcommittee on Transportation, Aviation, and Materials and the Subcommittee on Science, Research and Technology on H.R. 145 at the beginning of the 100th Congress continued to focus on the role of NSA oversight in computer security among the Federal agencies.

Donald Latham, Chairman of the National Telecommunications and Inforamtion Systems Security Committee (NTISSC) and Lt. General William Odom, Director of the National Security Agency, testified at the February 26, 1987 hearings on the role of the NSA, the function of NSDD-145, and the form of technical assistance

which the defense and military security agencies provide for the Federal Government. Also on February 26, 1987, Raymond Kammer, Deputy Director of the National Bureau of Standards, testified before the two Subcommittees on the role of NBS and his position on NTISS Directive No. 2 and its effect on Federal information security.

Mr. Latham's statement before the House Subcommittees outlined the role of NSA under NSDD-145. Mr. Latham stated that the civilian agencies are represented on two committees created under NSDD-145. These include the Systems Security Steering Group which consists entirely of civilian members of the President's Cabinet (see table 1), which sets overall information security policy for Federal agencies, and the National Telecommunications Information Systems Security Committee (NTISSC) (see table 2 for membership), under which NSA is the National Manager and assists NTISSC in implementing actual Federal computer security. Mr. Latham stated during questioning from Subcommittee Members:

TABLE 1.—SYSTEMS SECURITY STEERING GROUP

Chairman: The Honorable Frank C. Carlucci, Assistant to the President for National Security Affairs.

Executive Secretary: Lieutenant General William E. Odom, USA, National Manager for Telecommunications and Automated Information Systems Security.

Member: The Honorable George P. Shultz, Secretary of State; The Honorable James A. Baker III, Secretary of the Treasury; The Honorable Caspar W. Weinberger, Secretary of Defense; The Honorable Edwin Meese III, Attorney General; The Honorable James. C. Miller III, Director, Office of Management and Budget; and Robert Gates, Acting Director of Central Intelligence.

TABLE 2.—NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NTISSC)

Chairman: The Honorable Donald C. Latham, Assistant Secretary of Defense C^3I.

Executive Secretary: John C. Wobensmith.

Members: NSC, Department of State, Department of the Treasury, Department of Defense, Office of Management and Budget, Department of Justice, Department of Commerce, Department of Commerce, Department of Transportation, Department of Energy, Director of Central Intelligence, General Services Administration, Office of the Joint Chiefs of Staff, Department of the Army, Department of the Navy, Department of the Air Force, United States Marine Corps, National Security Agency, Defense Intelligence Agency, Federal Bureau of Investigation, Federal Emergency Management Agency, and National Communications System.

Observers: Federal Communications Commission, Intelligence Community Staff, Defense Communications Agency, National Aeronautics and Space Administration, Nuclear

Regulatory Commission, Chairman, SAISS, and Chairman, STS.

The Steering Group is chaired by the Assistant to the President for National Security Affairs and then is composed of all civilians from various cabinet level departments that are on the Steering Committee—Treasury, Defense, State, and so on—so that there is, in fact, at the very top of the NSDD-145 structure a group of cabinet level civilians who actually operate the mechanisms that are laid out in 145.

General Odom, in his testimony before the Subcommittee, described the role of the Department of Defense's National Computer Center and the services this Center provides both military and civilian agencies in the Federal Government. Under NSDD-145, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C^3I) chairs NTISSC.

Both Mr. Latham and General Odom, while testifying on the respective roles of NSA and DOD, stated that their main concern with an enhanced role for NBS, as outlined in H.R. 145, would be to duplicate efforts in computer security in the Federal Government. Both Mr. Latham and General Odom praised the role of NBS in providing standards for Federal computer systems, including security. However, both felt that many of the responsibilities outlined for NBS under H.R. 145 are identical to the responsibilities already provided for under NSDD-145, and that NSA and DOD currently are handling these responsibilities capably. In response to a question on how the respective roles of NSA and NBS might be affected under H.R. 145, General Odom stated:

Well, it is my general impression that it would give NBS responsibility for a lot of things we are now doing and would essentially build a duplication, presumably for two different sectors. In other words, you're building computers that are secure for civilian agencies, non-military or intelligence activities, and you would be securing computers or developing a program for those in the Defense Department.

However, despite the concern for duplication and potential overlap of computer security technology and services, there are those who are still concerned that civilian and defense and military computer security policies in the Federal Government should be separated. Specifically, there is concern that, for the sake of a unified Federal computer security policy, the military and defense would gain preeminence over Federal civilian agencies. Representative Glickman stated in his opening remarks before the first panel of witnesses.

* * * the basic concept of this bill, civilian preeminence in determining standards for classified information is the heart of what we are trying to do, not military preeminence * * *

Raymond Kammer, Deputy Director of the National Bureau of Standards, commented on the role of NBS in setting Federal computer security, particularly the role of the Institute of Computer

Sciences and Technology at NBS in developing a civilian telecommunications and computer security program. Mr. Kammer stated that he believed that H.R. 145, rather than causing duplication between NBS and NSA, complemented the two agencies. According to Mr. Kammer:

> The bill removes the potential for conflict between the Department of Commerce and the Director of the National Security Agency (NSA) in his capacity as National Manager under National Security Directive 145 (NSDD 145). Conflict has not yet arisen because the level of cooperation between NBS and the National Manager to develop security standards has been satisfactory. We have worked well together.

Mr. Kammer emphasized that there are some technical skills which NSA has which NBS does not have, nor is likely to acquire. Mr. Kammer also responded to questioning on the NBS budget by stating that a larger program involving reimbursable funding, in which Federal agencies pay NBS directly for services contracted out, would be an appropriate method for increasing the Federal civilian computer security budget at NBS.

David Pronko, President of PE Systems, a supplier of encryption devices for both military and private sector communications, added a private sector viewpoint. He was asked to characterize the relative strengths and weaknesses of NSA and NBS with respect to providing security for military and civilian computers. He said:

> From the communications security point of view, I feel that NSA has—my own personal view—a much more pragmatic approach and a more methodical approach on handling the communications security. At NBS, you have really more of a laissez faire approach to it, and here again, it is probably brought about by private industry working within that system.

INFORMATION PRIVACY AND SECURITY

During the Subcommittee hearings of the 99th Congress, several questions were raised about a possible "sensitive but unclassified" categorization of Federal information. when NTISS Directive No. 2 was issued in late 1986, providing a mechanism for a "sensitive but unclassified" category, interest and concern both in the Federal Government and in the private sector grew.

This concern was voice by several witnesses during the hearings on February 26, 1987. The definitions of "sensitive but unclassified" used in NTISS Directive No. 2 and in H.R. 1454 initially appear similar. H.R. 145 defines "sensitive" information as "any information, the loss, misuse, or unauthorized access of which could adversely affect the national interest or the conduct of Federal programs . . ." NTISS Directive No. 2 cited that "sensitive" information is that information in which the "disclosure, loss, misuse, alteration, or destruction could adversely affect national security or other Federal Government interests." But NTISS Directive No. 2 goes on to add that government interests may be those related, but not limited to:

> . . . the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

This additional range of activities, along with the intent of classifying this information as "sensitive", concerned many witnesses during the hearings on H. 145. Mr. Kammer of NBS stated:

> The definition of sensitive data that's contained in the Poindexter Directive is a totally—in my point of view, at least—is a totally inclusionary definition. There is no data that anyone would spend money on that is not covered by that definition. Therefore, civil data is covered; therefore, the Brooks Act and the Privacy Act are either in conflict with it, or one is superior to the other.

One group of witnesses which responded to the definition of "sensitive" information during the hearings on February 26, 1987 included Jack Simpson, President of Mead Data Central, Inc.; Kenneth Allen, Senior Vice President, Government Relations, Information Industry Association; Ms. Ceryl Helsing, Information Security Manager, Bankamerica Corporation and Chairman, Data Security Committee, American Bankers Association; and Mr. Geoffrey Turner, Communications Security manager, Bankamerica Corporation. They raised concerns that NSA would apply the "sensitive but unclassified" categorization to commercial databanks (such as NEXIS), which provide a wide range of data on Federal Government policies and laws; as well as raising concerns about the role of NSA in recertifying the Data Encryption Standard (DES), a method of encrypting data in information systems, developed by NBS. NSA had stated it would not recertify DES after 1988.

Many commercial databases are online services in which a user, gaining access to the database through a computer, can retrieve information on a wide variety of subjects. Corporations, news media, Federal, State and Local governments, and the legal, medical and accounting professions use these services for timely and current information. Providers of these services feel that restrictions on the type of information which may be made available to the general public will hurt that industry. Mr. Simpson stated in testimony:

> Such new restrictive and unwarranted policies and the unilateral control of the Defense Community threaten to bring this industry to a halt and would negate the significant productivity gains being made in many sectors of our economy including legal, financial, government, medical, and the scientific and technological community.

Mr. Simpson and others also stated that they were not opposed to the restriction of classified data by the national security and defense communities in the Federal Government. But Mr. Simpson stated that no "magical transformation" occurs when unclassified data is entered into a computer; if it is already unclassified in print form, it does not become more important or crucial because it is entered into a computer database. Mr. Simpson opposed the "sensi-

tive" categorization in NTISS Directive No. 2, and supported H.R. 145 during testimony.

The failure to recertify DES and NSA also was criticized by several witnesses during the February 26, 1986 hearings. Failure to recertify is seen by many in the private sector as an attempt by NSA to infringe on a security process for transmitting data. Mr. Turner, commenting on the ability of Bankamerica to safely and expeditiously transfer funds through DES, claimed that a failure to recertify by NSA has led to a "slowdown" in the security of electronic funds transfer and further encryption technology development and use in the financial community. Ms. Helsing also echoed these concerns, and strongly supported the concept of a Computer Security and Privacy Advisory Board, with some minor changes, as recommended by H.R. 145, as a formal measure for private sector communication with the Federal Government on such issues as data encryption.

Other witnesses were concerned that an expanded "sensitive but unclassified" definition would impinge upon personal liberties, as well as the free flow of information vital to scientific and industrial development. Mr. Jerry Berman of the American Civil Liberties Union, and Mr. John Richardson of the Institute of Electrical and Electronics Engineers, testified during the 100th Congress on this issue.

Mr. Berman, in his opposition to NSDD-145 and NTISS Directive No. 2, testified that currently there are statutes which protect classified information from disclosure: "If it's classified, protect it. If it's proprietary, trade secrets, there are statutes on the books." Mr. Berman stated that a broad and vague definition would lead to a restriction of information, less free access to information, and less right to know, and he supported H.R. 145 for passage into law. Mr. Berman also stated that since NSA has no public charter, that statutory power to NSA for categorizing sensitive information would lead to a situation in which citizens would not have redress to overturn decisions restricting sensitive information.

Mr. Richardson, also testifying on February 26, 1987, opposed NTISS Directive No. 2, and supported H.R. 145, because of concerns which the IEEE has that a new categorization of information as sensitive might restrict the free flow of information vital to U.S. economic survival. Mr. Richardson stated:

> The IEEE thinks, in this regard, that the unabridged dissemination of unclassified scientific and technical information is crucial for the continued advancement of U.S. industry, and we oppose restraints on its exchange.

Mr. Richardson stated that such exchanges would be severely restricted under NTISS Directive No. 2. He stated that both government and non-government information might qualify for this classification, and supported H.R. 145 as an alternative to separate the protection of computer systems which deal with national security information, from those computer systems dealing with non-national security information. Mr. Richardson also expressed some dissatisfaction with the definition of "sensitive" as outlined in H.R. 145, believing that it was, like the NTISS definition, too broad and general.

These witnesses, representing a variety of perspectives and concerns, felt that NTISS Directive No. 2, with its expanded definition of "sensitive" data, would impair the use of data bases, the ability to encrypt data, the protection of civil liberties, and the free flow of scientific and technical information. All supported the general intent of H.R. 145. The subsequent rescinding of NTISS Directive No. 2 in March, 1987, resulted in part from this opposition over the nature and intent of this directive.

TRAINING FOR FEDERAL COMPUTER SYSTEMS USERS

Testimony from the hearings during the 99th Congress emphasized the need for greater training of personnel responsible for computer security training of personnel in the Federal Government. GAO, ABA, the Inspector General of HHS, and others commented on the current state of Federal computer training during the course of the Subcommittee on Transportation, Aviation and Materials hearings.

H.R. 2889, as introduced by Representative Glickman during the 99th Congress, would have established a focus within the Federal Government at the National Bureau of Standards for computer security research, and development of computer security guidelines. The intent of this provision was to ensure that agencies would better train personnel in the vulnerabilities of computer and communication systems. On the last day of testimony before the two subcommittees on October 30, 1985, witnesses dealt directly with H.R. 2889 and the need for Federal computer security training.

There is little argument that such training is needed or that in some areas, that much is needed to supplement existing training procedures. Most of the witnesses testifying on the current state of Federal computer security commented that computer security training the Federal Government is either inadequate or nonexistent and that such training is necessary. William Franklin, Associate Director, Information Management and Technology Division, GAO, stated on October 30:

> There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage, processing and transmission.

However, there was concern that the creation of a new structure within the Federal Government might add unnecessarily to its overall cost and bureaucracy. Several witnesses stated that existing Federal computer training facilities, such as those at NSA, should be used to train Federal employees. Robert Brotzman, Assistant Director for Computer Security at the National Computer Security Center at NSA, described the security program at the Computer Security Center. This program assists civilian and military agencies, as well as outside contractors with sensitive data, to develop secure information and communication systems. As Mr. Brotzman stated:

> The knowledge base that we have now will support an effective training program, and it will support the substan-

> tial improvement in the security of computer systems operated by and for the United States Government.

James Burrows, Director, Institute for Computer Sciences and Technology (ICST), of the NBS, spoke on the computer training and security programs at the ICST. As part of its mandate to develop computer security standards and guidelines, the ICST assists Federal agencies in developing computer security programs. This includes both software and hardware development, system interfaces, personal identification and authentication of users. The Department of Commerce opposed the structure of H.R. 2889 because of its interpretation that the Brooks Act and other legislation makes a Federal computer training and awareness mandate for NBS unnecessary. However, Mr. Burrows did state that NSDD–145 could be "slightly confusing in who has control" of overall Federal security management among the agencies. Mr. Burrows also stated that, to date, NSDD–145 has had little adverse effect on NBS' activities in computer security and training.

Several of the witnesses did speak in favor of Federal computer training legislation, although they also suggested changes in the language and intent of H.R. 2889. Donn Parker, a computer crime and security expert at SRI International, also spoke on October 30 on computer security in general, while testifying on H.R. 2889. Mr. Parker made several observations: that it is the information, not the technology, which needs security; that information must be considered secure before it goes into the computer; that technology controls to date are adequate—it is the management of "human controls" which need improvement; that most information systems employees consider security a detriment to productivity; therefore, that measures must be taken to incorporate computer security into personnel performance evaluations; that each individual must be held accountable for taking security precautions, to ensure that these measures are taken; that advisory and counseling provisions within an organization can short-circuit the stresses and problems which may drive someone to commit a computer crime; that all information systems workers, not just computer programmers, should be trained in securing systems; and that training should be broadened to include a wider range of potential vulnerabilities, including the full civil, military, and private sector prospectives of computer training and awareness.

William Franklin of GAO also addressed H.R. 2889:

> We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research program in the Federal Government and the requirement that each Federal agency provide mandatory periodic training in computer security.

Testimony during the 100th Congress also touched upon the current state of computer security and the need for training of Federal employees. This issue was discussed specifically during the May 19, 1987 testimony by GAO of its investigation of the computer security policies of nine Federal agencies. Other witnesses, during the hearings on February 26, 1987, on H.R. 145, stated that the overall responsibility for civilian Federal computer security policies

should rest in the civilian agencies. Under H.R. 145, the focus for training civilian Federal agency personnel for computer security again would be placed with the National Bureau of Standards. The need for a strong computer security training program for Federal employees is still seen as a necessary and vital aspect of ensuring Federal computer security.

David Pronko, President of PE Systems, responded to a question about whether NSA or NBS could provide the training envisioned in H.R. 145.

> At this stage, from what I've seen and in my earlier comments, I'm not sure either has a leg on the other as far as the computer security training right now. It seems that the NSA within the last few years has gained a foot hold in that arena, due to their programs.

III. Need for Legislation

There are several key principles the Committee seeks to emphasize by this legislation:

1. Computer crime in the Federal Government appears to be much more pervasive and serious an issue than previously assumed. Descriptions of computer criminals as "insiders" by ABA, GAO, the Inspector General of HHS, and others may imply that many Federal computer users represent potential risks of fraud and abuse.

2. Security measures in a number of agencies are very vulnerable to abuse and fraud. Only five of 25 Federal computer systems surveyed by GAO contained minimum safeguards, and only two of 25 systems offered formal training sessions for computer users.

3. There is a need for coordinated guidance for security of sensitive information in computers. There is a perception that NSDD-145 could further complicate a situation which already is unclear; that is, Federal agencies are currently required to follow existing laws and regulations, such as the Brooks Act, the Paperwork Reduction Act, and the OMB circular, to set guidelines and standards for computer security.

4. NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. Although the Administration has indicated its intention to address this issue, the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data.

5. Training of Federal personnel in ADP security is a critical issue to ensure security in Federal agencies. Yet many Federal agencies do not take advantage of available training to remedy this problem. A stronger, more active computer training and awareness program is needed to address this issue in the civil agencies of the Federal Government.

6. Greater emphasis should be given to cooperation between the military and civil agencies as well as the private sector in setting computer security and training goals. This can be accomplished by fostering greater communication and cooperation between the NBS and NSA in setting overall Federal computer policy.

IV. Explanation of the Bill

PURPOSE

The purpose of H.R. 145, the Computer Security Act of 1987, as amended, is to improve the security and privacy of sensitive information in Federal computer systems. It achieves this purpose through improved training, aimed at raising the awareness of Federal workers about computer system security, by establishing a focal point within the government for developing computer system security standards and guidelines to protect sensitive information, and by requiring agencies to establish computer system security plans.

To explain what these mean, it is first necessary to examine several underlying concepts that define and scope the boundaries of the bill's coverage. First, the primary objective of the bill is controlling unauthorized use of the information in Federal computer systems, rather than merely protecting the computer systems themselves. Although computer hardware and software have real value and certainly must be safeguarded, it is the data stored, manipulated, displayed and transmitted by computer systems that represent the greatest vulnerability. Nevertheless, computer systems are the instrumentality through which security measures are usually applied. Therefore, the bill makes distinctions both about which computer systems are included as well as about what kinds of information are subject to the bill's provisions.

Second, the term "computer system" as used throughout the bill is defined to be essentially identical to the term "automatic data processing equipment" in Section 111 of the Federal Property and Administrative Services Act of 1949 (Brooks Act). A computer system is described structurally to include traditional hardware (computers and ancillary equipment), software, firmware, procedures for use of the system by people, services intended to provide support to the operation of the system, and related resources as defined in regulations issued by the Administrator of General Services. A computer system is also described functionally to include any equipment or interconnected system or subsystems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

The term "federal computer system" is used to delineate the reach of the bill to include federal agencies, contractors of federal agencies, and other organizations that process information using a computer system on behalf of the federal government to accomplish a federal government function. The latter category is limited to cases where there is a direct federal interest. Examples would include state agencies that disburse federal funds, monitor compliance with federal regulations on behalf of the federal government, collect statistical information for the purpose of federal funding decisions, or act in some other way as a direct extension of the federal government. The measures used for protecting sensitive information in such cases, just as elsewhere, must be cost effectively applied and commensurate with the risk and magnitude of harm. The term "operator of a federal computer system" denotes an agency or

institution that owns or otherwise possesses a federal computer system, rather than an individual who physically operates the machine. The term "sensitive information" is used to limit the kinds of information which are covered by the bill. It is intended to guide the National Bureau of Standards as to the kinds of information it should address in the standards development process. It is not intended to authorize establishment of a formal new category of information. (See discussion on Rules of Construction.) Sensitive information is defined as unclassified information which, if lost, misused, accessed or modified in an unauthorized way, could adversely affect the national interest the conduct of federal programs or the privacy of individuals.* Examples include information which if modified, destroyed or disclosed in an unauthorized manner could cause:

Loss of life;
Loss of property or funds by unlawful means;
Violation of personal privacy or civil rights;
Gaining of an unfair commercial advantage;
Loss of advanced technology, useful to a competitor; or
Disclosure of proprietary information entrusted to the government.

The definition of sensitive information allows the possibility that some unclassified information may not be sensitive. Each operator of a federal computer system must make a determination (as described later) as to which unclassified information in its possession is sensitive. Sensitive information does not include nor does the bill apply to classified information for which extensive standards-setting authority already exists. These mechanisms are unaffected by H.R. 145.

ADDITIONS TO NBS ORGANIC ACT

H.R. 145 amends the Act of March 3, 1901, creating the National Bureau of Standards, to add the mission of developing standards, guidelines and associated methods and techniques for computer systems to the list of authorized activities of the agency. The reason for this language is to provide specific authorization for activities that are widely acknowledged as necessary in the computer age, but which are conducted currently under general authorities contained in the Act. It is intended to authorize NBS to study the means of automatic computation (computer science) independent of the technology involved. Therefore, this clarification of NBS' Organic Act sets out the NBS mission in computer science in general and does not focus on computer security.

The bill also adds three new sections to the Act of March 3, 1901. Section 20 provides a hierarchy enumeration of NBS' responsibilities. At the top of the hierarchy is the mission of developing standards, and associated methods and techniques for computer systems generally. An example would be the "Open Systems Interconnection" (OSI) standards for computer networking, which the Bureau develops technically (with extensive private sector input) and pre-

* But which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

sents to the American National Standards Institute, and through it to the International Standards Organization, for adoption. This statement of responsibility is intended to conform Section 20 with the above addition to the list of authorized activities.

At the next hierarchical level NBS is responsible for developing uniform standards and guidelines, in all areas other than security, for federal computer systems. As before, this delineation of responsibility is intended to conform Section 20 and to provide specific authority for activities that are currently carried out under general provisions of the Organic Act. The product of this effort is the Federal Information Processing Standards (FIPS) which are used government-wide.

In current practice, some computer standards developed by NBS become compulsory under authority of OMB pursuant to the Brooks Act and the Paperwork Reduction Act. The process outlined in H.R. 145—which includes standards development by NBS and subsequent promulgation by the Secretary of Commerce under redrafted authority in the Brooks Act (to be described later)—is essentially the same as current practice, but is spelled out more explicitly.

Systems involving intelligence activities, cryptologic activities related to national security, direct command and control of military forces, equipment that is integral to a weapons system or direct fulfillment of military or intelligence missions (except routine administrative and business functions) are exempted from this provision. Such systems are highly specialized in their functions and have been traditionally exempted from government-wide standards and regulations applying to general purpose computer systems. Therefore, the boundary of NBS' responsibility for non-security standards is drawn so as to exclude such defense-related, special-purpose systems.

The third hierarchial level spells out explicitly, and thereby gives special emphasis to, responsibility for standards and guidelines in the computer security arena. It assigns to NBS responsibility within the federal government for developing technical, management, physical, and administrative standards and guidelines designed to achieve, in a cost-effective way, the security and privacy of sensitive information in federal computer systems. The purpose of the standards and guidelines is to control loss and unauthorized modification or disclosure of sensitive information and to prevent computer-related fraud and abuse.

Certain computer systems are exempted from this provision, regardless of the kind of information they contain. There are two categories of such exempted systems. The first is the same list of defense and intelligence-related systems that were exempted in the previous subsection, dealing with non-security standards. The second category includes systems that are operated at all times under rules designed to protect classified information. The chief effect of this exemption is to exclude classified systems from coverage by this subsection of the bill. Also exempted are mixed systems—those systems containing classified information at certain times and unclassified information at other times—provided such systems are operated at all times under the rules for protecting classified information. The purpose of this exemption is to avoid

imposition of a second, less stringent set of security standards—the NBS standards—for the unclassified operations of a mixed system. Further relief for mixed systems is provided in the amendment to the Brooks Act, allowing system operators to employ standards, other than the NBS standards, if such standards are more stringent. For example, an operator of a mixed system might use a subset of the classified rules for his unclassified operations, if the subset were more stringent than the NBS standards.

One reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive-145. As indicated previously, this directive established an interagency committee—the National Telecommunications and Information Systems Security Committee (NTISSC). The function of the NTISSC is to devise operating policies needed to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive government national security information. Policies developed by NTISSC would apply government-wide.

While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information". For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting policy with regard to unclassified information. In so doing, the bill has the additional effect of specifically limiting the purview of the NTISSC to systems containing classified information and cancelling the authority contained in NSDD-145 for systems containing unclassified information. NBS is required to work closely with other agencies and institutions, such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS.

Note that the previous subsection dealt with developing non-security standards and guidelines, most of which affect hardware and software performance and interfaces. Accordingly, the bill's jurisdiction in that area is defined by the universe of federal computer systems, as limited by certain exceptions. In this subsection, the bill deals with security standards and guidelines, which apply more properly to protecting information. Therefore, the bill addresses unclassified (but sensitive) information in federal computer systems, but with certain systems exempted.

The method for promulgating federal computer system security standards and guidelines is the same as for non-security standards and guidelines. NBS submits them to the Secretary of Commerce along with recommendations regarding the extent to which they should be made compulsory and binding. The Secretary of Commerce, under redrafted authority in the Brooks Act (to be explained later), then promulgates standards and guidelines, making those standards compulsory and binding that he determines are

necessary to improve the efficiency of operation or security and privacy of federal computer systems.

An additional responsibility of NBS is to devise guidelines for use by agencies in training employees in security awareness and good security practice. Section 5 of H.R. 145 requires each Federal agency to provide for the training of certain employees of each operator of a Federal computer system that is within or under the supervision of that agency.

Also, as part of its responsibility for developing computer standards and guidelines, NBS is required to devise validation procedures to evaluate the effectiveness of the standards and guidelines. This is not an enforcement or compliance determining function. Rather, it provides the ability for operators to determine if the standards and guidelines are achieving their desired purpose. NBS is to maintain liaison (as it now does) with users of the standards, to assure their workability.

In fulfilling these responsibilities, NBS is authorized to give technical assistance to the General Services Administration, the Office of Personnel Management, operators of federal computer systems and the private sector in implementing the standards and guidelines promulgated pursuant to the bill. Also, NBS is authorized to perform research and conduct studies to determine the nature and extent of the vulnerabilities of computer systems and to devise techniques to protect, in a cost effective way, the information contained in them, and to coordinate with other agencies (including NSA) which perform such research, to gain the benefits of their efforts.

Finally, in carrying out its responsibilities to develop standards and guidelines for protecting sensitive information in federal computer systems and to perform research, NBS is required to draw upon technical security guidelines developed by the NSA to the extent that NBS determines that NSA's guidelines are consistent with the requirements of civil agencies. The purpose of this language is to prevent unnecessary duplication and promote the highest degree of cooperation between these two agencies. NBS will treat NSA technical security guidelines as advisory, however, and, in cases where civil agency needs will best be served by standards that are not consistent with NSA guidelines, NBS may develop standards that best satisfy the agencies' needs.

It is important to note the computer security standards and guidelines developed pursuant to H.R. 145 are intended to protect sensitive information in Federal computer systems. Nevertheless, these standards and guidelines will strongly influence security measures implemented in the private sector. For this reason, NBS should consider the effect of its standards on the ability of U.S. computer system manufacturers to remain competitive in the international marketplace.

A new Section 21 of the NBS Organic Act establishes a twelve-member Computer System Security and Privacy Advisory Board within the Department of Commerce. The chief purpose of the Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administra-

tive and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.

Members of the Board are to be appointed by the Secretary of Commerce and are to come from both inside and outside the federal government and have qualifications as specified in the bill.

Specifically, the Board's complement is basically divided between federal government and non-federal government members.

The non-federal government segment is further divided into two sub-entities, namely, (1) industry and (2) technology or other related disciplines.

The industry segment is intended tobe for hardware, and/or software producers and systems integrators; at least one of whom is representative of small or medium sized companies, and one of whom is representative of a large company.

The technology or other related disciplines segment could include those eminent in academia, as well as the private sector producers of data bases, the financial community and other sophisticated users of the technology. Members will not be paid for their services, other than for reimbursement of travel expenses. The Board may use personnel from NBS or other agencies of the federal government for the purpose of staff support, with the consent of the respective agency head.

The Board may conduct business with as few as seven members present. Findings must be reported to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of Congress.

Section 23 is a housekeeping change. It adds a short title to the NBS Organic Act for ease of reference.

AMENDMENT TO THE BROOKS ACT

H.R. 145 contains a redrafted version of section 111(d) of the Federal Property and Administrative Services Act of 1949. The chief purpose is to establish an orderly process for promulgating standards and guidelines pertaining to Federal computer systems. Specifically, the Secretary of Commerce is charged with issuing standards and guidelines based on the standards and guidelines developed by NBS, pursuant to two subsections in the amendment to the NBS Act. As explained, those subsections formalize NBS' responsibility for developing both non-security and security standards and guidelines. The Secretary is authorized to make certain standards compulsory and binding as needed to improve the efficiency of operation or security and privacy of federal computer systems. The President may disapprove or modify the standards and guidelines if he determines such action to be in the public interest.

As described earlier, the amendment contains relief from strict compliance with these standards, when agencies already employ standards that are more stringent. An example is the instance where the unclassified operations of a mixed system are conducted under a subset of the rules used during classified operations, pro-

vided the subset is tougher than the standards mandated by the Secretary.

Further relief is provided by language authorizing the Secretary of Commerce to waive the compulsory standards when compliance would adversely affect an operator's mission or cause major financial impact on the operator that is not offset by government-wide savings. The Secretary may delegate this authority to agency heads when necessary and desirable to achieve timely and effective implementation of measures to improve federal computer system security and privacy. Agencies heads may redelegate this authority only to certain high level officials, designated pursuant to the Paperwork Reduction Act for the purpose of carrying out the agencies' information management activities under that Act.

The need for delegation authority arises from Committee concerns about the administrative burden on NBS. Under normal procedures, the Secretary can be expected to rely on NBS for technical evaluation of any requests for waiver. The Committee expects NBS to devote the bulk of its energy to producing computer systems standards, rather than to such compliance determinations. Accordingly, the amendment to the Brooks Act allows the Secretary flexibility to delegate the waiver authority.

The amendment ties the process for developing and promulgating computer system standards to the requirement for an integrated information resources management system, as set forth in the Paperwork Reduction Act. To achieve this, the Administrator of General Services is charged with developing and implementing policies on federal computer systems and revising the federal information resources management regulations to reflect the standards and guidelines emanating from the Secretary of Commerce.

TRAINING

One of the fundamental purposes of H.R. 145 is improved computer security awareness and use of accepted computer security practice by all persons involved in management, use, or operation of federal computer systems that contain sensitive information. As indicated, the Committee found in its hearings that training in these areas is a particular weakness at most agencies. A GAO study revealed, for example, that only two of twenty-five major federal computer systems surveyed had adequate training programs. For this reason, the bill contains a requirement that each Federal agency provide for the periodic training of all employees involved with the management, use or operation of each Federal computer system within or under the supervision of that agency. The objectives of the training are to enhance employees' awareness of the threats and vulnerabilities of computer systems and to encourage the use of improved security practices.

The process envisioned in the bill starts with NBS, which is responsible for developing training guidelines based on its research and study of vulnerabilities and countermeasures. Within six months of enactment and using these guidelines, the Office of Personnel Management must issue regulations covering such areas as training objectives for various categories of employee, general guidance concerning course content and frequency of training. Strictly

speaking, the regulations issued by OPM under this section apply only to Federal civilian employees. The overall effect of the section, however, is to extend the regulations' applicability to employees of all operators of a Federal computer system as defined in the bill. The bill specifies that training begin within 60 days after the issuance of regulations by OPM. Each Federal agency is responsible for making provisions for the training of its own employees as well as those of contractors and other organizations that it supervises. Training should be tailored to the particular operating conditions and needs of each operator. Agencies may provide for the training in a variety of ways. For example, an agency may use its internal training capabilities or the services of training providers such as OPM or private companies. For the employees of contractors and other organizations under the supervision of an agency, the agency may use any available contractual or management instrument to require the operator to conduct periodic training in accordance with the NBS training guidelines and the OPM regulations. In so doing, the Committee expects that the agency will require the operator to bear the costs associated with furnishing the training. An agency head may approve an alternative training program which he determines to be at least as effective in accomplishing the objectives of the NBS guidelines and OPM regulations.

SECURITY PLANS

A key determination upon which many provisions of the bill depend is the identification of which Federal computer systems contain sensitive information. By definition, the search for such systems is restricted to systems containing unclassified informataion. Some, but possibly not all, of these systems will be determined to contain unclassified-sensitive information. The philosophy refected in the bill is that each Federal agency is best equipped to make that determination relative to its own mission and circumstances. Therefore, the bill calls on each agency to make a determination for each computer system under its control, within six months of enactment. The determination should be based on the definition of "sensitive" contained in the bill and use the additional guidance in the section on purpose in this report.

Within one year of enactment, each agency must also establish a plan for the security and privacy of each computer system so identified. Plans are to be based on the standards and guidelines issued by the Secretary of Commerce pursuant to the Brooks Act, or any waivers received. This requirement applies only to those computer systems subject to the provision of that Act. Plans are also to be commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information being protected. Copies of the plans must be submitted to the National Bureau of Standards and the National Security Agency for advise and comment and to the Office of Mangement and Budget, which has the authority to disapprove the plan.

Implicit in the authority to disapprove security plans is responsibility for oversight of the identification process and compliance with the security plans as approved. Thus, OMB is the watchdog over the key implementation step in the bill.

RULES OF CONSTRUCTION

The purpose of this section is to make it explicitly clear that the Computer Security Act has no bearing on the public availability or use of information. The designation of information as sensitive [or as subject to protection] under the Computer Security Act is not a determination that the information is not subject to public disclosure.

The Computer Security Act is strictly neutral with respect to public disclosure of information. Any information that was required to be disclosed under the Freedom of Information Act or other laws before enactment of the Computer Security Act will still have to be disclosed after enactment. Requests for information that was previously subject to withholding and that continues to qualify for withholding may be denied.

Also, the Act may not be construed to expand the authority of any Federal agency to limit, restrict, regulate, or otherwise control the collection, maintenance, disclosure, use, transfer, or sale of (1) any privately-owned information; (2) any information disclosable under the Freedom of Information Act or other law requiring or authorizing the public disclosure of information by Federal agencies; or (3) any public domain information. This restriction on government authority applies regardless of the medium in which the information may be maintained. For example, in recent months, interest has been expressed by some Federal officials in restricting or monitoring use of unclassified, private sector computerized databases such as LEXIS and NEXIS. This section makes it explicitly clear that no such authority is granted to agencies by the Computer Security Act.

V. Sectional Analysis—H.R. 145

Section 1. Short Title.

Section 2. Purpose: Sets forth the Congressional declaration that improving the security and privacy of federal computer systems is in the public interest and states Congressional intent to institute a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

The specific purposes of the Act are to assign the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems drawing upon the technical advice and assistance of the National Security Agency, where appropriate; to provide for promulgating such standards and guidelines through the Federal Property and Administrative Services Act of 1949; to require all operators of Federal computer systems that contain sensitive information to establish security plans; and to require mandatory periodic training for all persons involved in management, use or operation of Federal computer systems that contain sensitive information.

Section 3. Establishment of Computer Standards Program. Amends the Act of March 3, 1901 to add to the mission of the National Bureau of Standards the study of computer systems, as de-

fined in section 20(d) of the NBS Act, and their use to control machinery and processes.

Inserts a new Section 20(a) stating the National Bureau of Standards shall:

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) above, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce, for promulgation under section 111 of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) above through research and liaison with other government and private agencies.

Inserts a new Section 20(b) authorizing the National Bureau of Standards to:

(1) assist the private sector in using and applying the results of the programs and activities under this section;

(2) make recommendations to, assist and coordinate with other Federal agencies, as appropriate, in carrying out this Act;

(3) provide, as requested, technical assistance to operators of Federal computer systems in implementing the standards and guidelines promulgated pursuant to this Act;

(4) perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

(5) coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and

Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget) to assure—

(A) maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to the maximum extent feasible, that standards developed by the National Bureau of Standards are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Inserts a new Section 20(c) that requires the National Bureau of Standards to draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

Inserts a new Section 20(d) that defines—

(1) the term "computer system" as—

(A) any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

(2) the term "Federal computer system" as a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(3) the term "operator of a Federal computer system" as a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(4) the term "sensitive information" as any information, the loss, misuse, or unauthorized access or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" as having the meaning given such term by section 3(b) of the Federal Property and Administative Services Act of 1949.

Inserts a new section 21(a) establishing a Computer System Security and Privacy Advisory Board, with a chairman to be appointed by the Secretary of Commerce and twelve members as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

(2) four members from outside the Federal Government who are eminent in the computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

Inserts a new Section 21(b) stating that the duties of the Board shall be:

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

Inserts a new Section 21(b) stating that the term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

Inserts a new Section 21(d) prohibiting the Board from acting in the absence of a quorum, which shall consist of seven members.

Inserts a new Section 21(e) stating that Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

Inserts a new Section 21(f) that authorizes the Board in carrying out its functions, to used staff personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

Adds a new Section 23 which establishes a short title for the Act of March 3, 1901, henceforth to be known as the "National Bureau of Standards Act".

Section 4. Amendment to the Brooks Act. Replaces Section 11(d) of the Federal Property and Administrative Services Act of 1949 with new language that:

(1) empowers the Secretary of Commerce, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a)(2) and (3) of the National Bureau of Standards Act, to promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation of security and privacy of Federal computer systems;

(2) authorizes the head of a Federal agency to employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards contain, at a minimum, the provisions of those applicable standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) provides that the standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or caue a major adverse financial impact on the operator which is no offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be promptly transmitted to the Committee on Government Operations of the House of Representataives and the Committee on Governmental Affairs of the Senate;

(4) directs the Administrator of the General Services Administration to revise the Federal information resources management regulations to be consistent with the standards and guidelines promulgated by the Secretary of Commerce; and

(5) defines the terms "Federal computer system" and "operator of a Federal computer system" as having the meanings given in section 20(d) of the National Bureau of Standards Act.

Section 5. Federal Computer System Security Training. Requires each Federal agency to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who ae involved with the management, use, of or operation of each Federal computer system within or under the supervision of that agency:

(1) Directs that training be provided in accordance with the guidelines developed by the National Bureau of Standards and in accordance with regulations issued by the Office of Personnel Management for Federal civilian employees; or

(2) Provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

Training under this section shall be started within 60 days after the issuance of the regulations. Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved security practices.

Directs that within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided and the manner in which such training is to be carried out.

Section 6. Additional Responsibilities for Computer Systems Security and Privacy. Directs that within 6 months after the date of enactment each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

Provides that within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

Section 7. Definitions. Defines the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" as having the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

Section 8. Rules of Construction of Act. States that nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

VI. Effect of Legislation on Inflation

In accordance with Rule XI, Clause 2(l)(4), of the Rules of the House of Representatives, this legislation is assessed to have no adverse inflationary effect on prices and costs in the operation of the national economy.

VII. Committee Oversight Findings and Recommendations

Pursuant to Rule XI, Clause 2(l)(3)(A), and under the authority of Rule X, Clause 2(b)(1) and Clause 3(f), of the Rules of the House of Representatives, the following statement on oversight activities is made:

The Committee's oversight findings are incorporated in the recommendations contained in the present bill and report.

VIII. Oversight Findings and Recommendations by the Committee on Government Operations

Pursuant to Rule XI, Clause 2(l)(3)(D), and under the authority of Rule X, Clause 2(c)(2), of the Rules of the House of Representatives, the following statement on oversight activities by the Committee on Government Operations is made:

The Committee's oversight findings are reflected in the recommendations contained in the bill as reported by that Committee and the accompanying report.

IX. Budget Analysis and Projecton

The bill provides for new authorization rather than new budget authority and consequently the provisions of Section 308(a) of the Congressional Budget Act are not applicable.

X. Congressional Budget Office Cost Estimate

Pursuant to Section 403 of the Congressional Budget Act of 1974 and Rule XI, Clause 2(l)(3) of the Rules of the House of Representatives, the report of the Congressional Budget Office follows:

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

1. Bill number: H.R. 145.

2. Bill title: Computer Security Act of 1987.

3. Bill status: As ordered reported by the House Committee on Science, Space, and Technology, May 20, 1987.

4. Bill purpose: H.R. 145 would require the National Bureau of Standards (NBS) to establish a computer security standards program for those computer systems subject to the Brooks Act. The bill directs NBS to develop government-wide standards and guidelines, training programs, and validation standards to evaluate the effectiveness of computer security standards; and to work with the National Security Agency (NSA) and other agencies in developing

these standards and guidelines and conducting research and studies. Based on recommendations submitted by the NBS, the Secretary of Commerce would be required to promulgate standards and guidelines for computer security. The bill would also establish a 13-member Computer System Security and Privacy Advisory Board composed of representatives of other federal agencies and the private sector.

Within six months after the date of enactment, H.R. 145 would require all federal agencies to identify each computer system that contains sensitive data. Each agency would be required to establish a plan for the security of each computer and related system previously identified within a year after the date of enactment, and to revise it annually as necessary. The bill also requires mandatory periodic training in computer security for all federal agency employees who manage, use or operate computer systems. Each federal agency would also be required to provide for similar training for certain employees of private contractors and other organizations, such as state and local governments, that process information on behalf of the federal government.

5. Estimated cost to the Federal Government: CBO estimates that enactment of this bill would cost NBS about $4 million to $5 million annually beginning in fiscal year 1988. Additional costs for planning and training in computer security by all agencies throughout the federal government would probably cost $20 million to $25 million in 1988 and $15 million to $20 million in each fiscal year thereafter. To the extent that this legislation would reduce fraud or other financial losses, some savings could also result from enactment of this bill. It is not possible to quantify these potential savings at this time.

Basis of Estimate: Under the National Security Decision Directive (NSDD) 145, which became effective in September 1984, the President gave the National Security Agency (NSA) responsibility for ensuring the security of all classified and certain other sensitive information transmitted by federal computers or telecommunications systems. If enacted, H.R. 145 would assign some of this authority to NBS, mainly in the area of unclassified data. Although under current guidelines it is expected that most federal agencies, with assistance from NSA, would have strengthened security efforts consistent with the directive, this bill would enhance the role of NBS and would also impose new requirements upon federal agencies and their contractors in the area of computer security.

National Bureau of Standards.—Assuming enactment of H.R. 145 and any necessary appropriations by October 1, 1987, the expanded role of NBS in computer security management and training is estimated to cost about $2 million annually beginning in 1988. Based on information from NBS, an estimated $2 million to $3 million annually may also be needed for research, beginning in 1988. This assumes that NBS would expand its management and oversight role, but would also receive assistance and information from the National Computer Security Center (NCSC) within the Department of Defense (DoD).

Government-wide computer security plans.—The level of computer security varies greatly among the approximately 80 federal entities, included about 1,300 different organizations that would be af-

fected by this legislation. The cost of identifying all sensitive computer systems and developing an appropriate plan for facility, application and personnel security would thus vary greatly from agency to agency, depending upon the agency's current level of security, the size and number of sites, and the resources and expertise available to implement this provision.

CBO has not been able to contact each major federal entity to determine the cost of identifying and developing these plans for computer security. Based on the information available, it is expected that most agencies would probably assign existing personnel and resources to this task in order to meet the one-year deadline imposed by H.R. 145. If approximately 10,000 plans were developed, each requiring about 1-2 works weeks of effort by agency personnel, and two and one-half work days of review by NBS, NSA, and the Office of Management and Budget (OBM), the cost spread among the various federal agencies would be $10 million to $20 million over the fiscal years 1988 and 1989.

Government-wide training.—Currently, training resources in the area of computer security are scattered throughout the federal government. A few civilian agencies, such as the Department of Energy, have developed their own computer security training for both classified and unclassified systems. Most agencies, however, send employees to commercial courses or those offered by other federal agencies, such as the General Services Administration (GSA), the Office of Personnel Management (OPM), the Department of Agriculture Graduate School, or NSA.

H.R. 145 would require mandatory training for all federal and contractor personnel who manage, use or operate computer systems. The cost of such training depends on the number of people involved and the kind of training provided. Based on information from a number of agencies, it is expected that roughly half of all government and contractor employees, or about 3 million employees, would initially receive some type of training as a result of the bill. Subsequently, training would be provided to most new employees, and retraining would be required only periodically.

It is expected that most training in the area of computer security would become decentralized, with each agency responsible for developing its own programs, although some centralized training for smaller agencies and in specialized program areas would remain. The NCSC has developed a data base of educational opportunities offered by government, universities and private sources that is available to agencies. Training courses are relatively expensive, however. They currently cost about $50 to $200 per day per person (not including development costs) and typically are offered to technical personnel who attend a three-to-five day session. In an effort to reduce training costs, NCSC is developing training packages that will be available on tape or film, sharply reducing the training cost per person.

Based on the information from NCSC, GSA, OPM, and OMB, CBO made a number of assumptions about the amounts and types of training that would be required as a result of enactment of H.R. 145. The resulting estimates provide a rough estimate of the possible additional cost of training, but should not be considered precise.

Within three years after the date of enactment, it is assumed that about 90 percent of the estimated 3 million employees affected by the bill would receive some type of computer security awareness training. Assuming the availability of training modules and other low-cost products, it is expected that the cost for this type of training would have no significant budget impact over and above the cost of maintaining good information systems, which is now the responsibility of each agency. It is estimated that about 10 percent of the 3 million employees, or 300,000, would require more formalized training. Assuming that about three-quarters of these individuals (about one-half from DoD) would haved received training under current law, then about 75,000 employees would likely require training as a result of this bill. Three days of specialized training, at an average cost of $100 per day, for 75,000 persons would cost $20 million to $25 million over several years. After the initial training, costs for retraining and training of new personnel are expected to cost about $5 million annually.

Finally, it is assumed that about 250 civilian employees would gradually be recruited and/or trained to evaluate the technical protection capabilities of industry and government-developed systems, and to train other agency personnel. This type of training, according to NCSC, takes two to three years. At an average cost of $60,000 per year, including overhead, it is estimated that this type of support staff would cost the federal government about $15 million annually, once fully implemented.

6. Estimated cost to State and local governments: H.R. 145 would require training in computer security for nonfederal as well as federal operators of computer systems that process data on behalf of the federal government. This requirement would include state or local governments that are involved in such activities as monitoring compliance with federal regulations, disbursing federal funds, and collecting or maintaining data for ultimate federal use. Based on information from the committee, these nonfederal operators would be expected to bear the cost of furnishing the training. Because no complete inventory of the relevant computer systems at the state and local level exists, it is not possible at this time to estimate with precision the costs to state and local governments of providing this training. Based on the limited information available, we expect that total costs incurred by state and local governments are likely to be less than $25 million annually.

7. Estimate comparison: None.

8. Previous CBO estimate: On May 4, 1987, CBO transmitted to the House Committee on Government Operations a cost estimate for H.R. 145, as ordered reported by that committee on April 7, 1987. The estimated cost of each version of H.R. 145 is the same.

9. Estimate prepared by: Carol Cohen.

10. Estimate approved by: C.G. Nuckols, for James L. Blum, Assistant Director for Budget Analysis.

XI. Administration Position

Executive Office of the President,
Office of Management and Budget,
Washington, DC, May 12, 1987.

Hon. Robert A. Roe,
Chairman, Committee on Science, Space, and Technology,
U.S. House of Representatives, Washington, DC.

Dear Mr. Chairman: I am pleased that through intensive consultations between the Administration and the Congress great progress has been made toward agreement on a Computer Security Act of 1987. I hope that this statement of Administration views will assists in offering constructive solutions to areas where further improvements are desirable.

As we have reviewed H.R. 145, a primary concern has been to assure that the roles of the National Bureau of Standards (NBS) and the National Security Agency (NSA) are discharged in a manner that will promote a sound public policy and result in efficient, cost effective, and productive solutions. In this regard it is the Administration's position that NBS, in developing Federal standards for the security of computers, shall draw upon technical security guidelines developed by NSA in so far as they are available and consistent with the requirements of civil departments and agencies to protect data processed in their systems. When developing technical security guidelines, NSA will consult with NBS to determine how its efforts can best support such requirements. We believe this would avoid costly duplication of effort.

Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review. In cases where civil agency needs will best be served by standards that are not consistent with NSA technical guidelines, the Secretary of Commerce will have authority to issue standards that best satisfy the agencies' needs. At the same time agencies will retain the option to ask for Presidential review of standards issued by the Department of Commerce do not appear to be consistent with U.S. public interest, including that of our national security. I am enclosing proposed changes to the present text of H.R. 145 which are consistent with the NBS-NSA relationship outlined above and make several minor changes that would further improve the bill.

In closing, I want to assure you that a reported bill within the parameters outlined in this letter will have the Administration's support.

Sincerely yours,

James C. Miller III, *Director.*

XII. Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omit-

ted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

ACT OF MARCH 3, 1901

AN ACT To establish the National Bureau of Standards

* * * * * * *

SEC. 2. The Secretary of Commerce (hereinafter referred to as the "Secretary") is authorized to undertake the following functions:

(a) * * *

* * * * * * *

(f) Invention and development of devices to serve special needs of the Government.

In carrying out the functions enumerated in this section, the Secretary is authorized to undertake the following activities and similar ones for which need may arise in the operations of Government agencies, scientific institutions, and industrial enterprises:

(1) * * *

* * * * * * *

(18) the prosecution of such research in engineering, mathematics, and the physical sciences as may be necessary to obtain basic data pertinent to the functions specified herein; [and]

(19) the compilation and publication of general scientific and technical data resulting from the performance of the functions specified herein or from other sources when such data are of importance to scientific or manufacturing interests or to the general public, and are not available elsewhere, including demonstration of the results of the Bureau's work by exhibits or otherwise as may be deemed most effective, and including the use of National Bureau of Standards scientific or technical personnel for part-time or intermittent teaching and training activities at educational institutions of higher learning as part of and incidental to their official duties and without additional compensation other than that provided by law[.]; and

(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.

* * * * * * *

SEC. 20. (a) The National Bureau of Standards shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer system; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to com-

puter systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureaus of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

(d) As used in this section—

(1) the term "computer system"—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

(2) the term "Federal computer system"—

(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the con-

duct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physicial safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

(c) The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of busi-

ness, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

(g) As used in this section, the terms "computer system" and "Federal computer system" have the meanings given in section 20(d) of this Act.

SEC. [20.] 22. Appropriations to carry out the provisions of this Act may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

SEC. 23. This Act may be cited as the National Bureau of Standards Act.

SECTION 111 OF THE FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949

AUTOMATIC DATA PROCESSING EQUIPMENT

SEC. 111. (a) * * *

* * * * * * *

[(d) The Secretary of Commerce is authorized (1) to provide agencies, and the Administrator of General Services in the exercise of the authority delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, and (2) to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under provisions of this subsection.]

(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published prompt in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Fed-

eral computer system with in or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

(5) As used in this subsection, the terms "Federal computer system" and "operator of a Federal computer system" have the meanings given in section 20(d) of the National Bureau of Standards Act.

* * * * * * *

XIII. Committee Recommendation

A quorum being present, the bill was ordered favorably reported on May 20, 1987, by unanimous voice vote.

○